COMPUTER MISUSE ACT (OF SINGAPORE)

PART I

PRELIMINARY

Short title

1. This Act may be cited as the Computer Misuse Act.

Interpretation

2. --(1) In this Act, unless the context otherwise requires --

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include --

(a) an automated typewriter or typesetter;

(b) a portable hand held calculator;

(c) a similar device which is non-programmable or which does not contain any data storage facility; or

(d) such other device as the Minister may, by notification in the Gazette, prescribe;

“computer output” or “output”means a statement or representation (whether in written, printed, pictorial, graphical or other form) purporting to be a statement or representation of fact --

(a) produced by a computer; or

(b) accurately translated from a statement or representation so produced;

"computer service" includes computer time, data processing and the storage or retrieval of data;

"damage" means, except for the purposes of section 13, any impairment to a computer or the integrity or availability of data, a program or system, or information, that --

(a) causes loss aggregating at least $10,000 in value, or such other amount as the Minister may, by notification in the Gazette, prescribe except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account;

(b) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of one or more persons;

(c) causes or threatens physical injury or death to any person; or

(d) threatens public health or public safety;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

"electronic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer;

"intercept" , in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof;

"program or computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

[21/98]

--(2) For the purposes of this Act, a person secures access to any program or data held in a computer if by causing a computer to perform any function he --

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner),

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

(3) For the purposes of subsection (2) (c), a person uses a program if the function he causes the computer to perform --

(a) causes the program to be executed; or

(b) is itself a function of the program.

(4) For the purposes of subsection (2) (d), the form in which any program or data is output (and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

(5) For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorised or done without authority if --

(a) he is not himself entitled to control access of the kind in question to the program or data; and

(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

(6) A reference in this Act to any program or data held in a computer includes a reference to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

(7) For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer --

(a) any program or data held in the computer concerned is altered or erased;

(b) any program or data is added to its contents; or

(c) any act occurs which impairs the normal operation of any computer,

and any act which contributes towards causing such a modification shall be regarded as causing it.

[S 92/97]

(8) Any modification referred to in subsection (7) is unauthorised if --

(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and

(b) he does not have consent to the modification from any person who is so entitled.

(9) A reference in this Act to a program includes a reference to part of a program.

PART II

OFFENCES

Unauthorised access to computer material

3. --(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.

[21/98]

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

[21/98]

(3) For the purposes of this section, it is immaterial that the act in question is not directed at --

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

Access with intent to commit or facilitate commission of offence

4. --(1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence.

[21/98]

(2) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.

[21/98]

(3) Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

[21/98]

(4) For the purposes of this section, it is immaterial whether --

(a) the access referred to in subsection (1) is authorised or unauthorised;

(b) the offence to which this section applies is committed at the same time when the access is secured or at any other time.

[21/98]

Unauthorised modification of computer material

5. --(1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to

imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

[21/98]

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

[21/98]

(3) For the purposes of this section, it is immaterial that the act in question is not directed at --

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

(4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.

Unauthorised use or interception of computer service

6. --(1) Subject to subsection (2), any person who knowingly --

(a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b),

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

[21/98]

--(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

[21/98]

(3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at --

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

Unauthorised obstruction of use of computer

7. --(1) Any person who, knowingly and without authority or lawful excuse --

(a) interferes with, or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding

$10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

[21/98]

--(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

[6A

[21/98]

Unauthorised disclosure of access code

8. --(1) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if he did so --

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) knowing that it is likely to cause wrongful loss to any person.

[21/98]

--(2) Any person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

[6B

[21/98]

Enhanced punishment for offences involving protected computers

9. --(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such an offence shall, in lieu of the punishment prescribed in those sections, be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 20 years or to both.

[21/98]

(2) For the purposes of subsection (1), a computer shall be treated as a “protected computer” if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for --

(a) the security, defence or international relations of Singapore;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or

(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.

[21/98]

(3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer, program or data attracts an enhanced penalty under this section.

[6C

[21/98]

Abetments and attempts punishable as offences

10. --(1) Any person who abets the commission of or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence.

(2) For an offence to be committed under this section, it is immaterial where the act in question took place.

[7

PART III

MISCELLANEOUS AND GENERAL

Territorial scope of offences under this Act

11. --(1) Subject to subsection (2), the provisions of this Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore.

(2) Where an offence under this Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore.

(3) For the purposes of this section, this Act shall apply if, for the offence in question --

(a) the accused was in Singapore at the material time; or

(b) the computer, program or data was in Singapore at the material time.

[8

Jurisdiction of Courts

12. A District Court or a Magistrate's Court shall have jurisdiction to hear and determine all offences under this Act and, notwithstanding anything to the contrary in the Criminal Procedure Code (Cap. 68), shall have power to impose the full penalty or punishment in respect of any offence under this Act.

[9

Order for payment of compensation

13. --(1) The court before which a person is convicted of any offence under this Act may make an order against him for the payment by him of a sum to be fixed by the court by way of compensation to any person for any damage caused to his computer, program or data by the offence for which the sentence is passed.

(2) Any claim by a person for damages sustained by reason of the offence shall be deemed to have been satisfied to the extent of any amount which has been paid to him under an order for compensation, but the order shall not prejudice any right to a civil

remedy for the recovery of damages beyond the amount of compensation paid under the order.
(3) An order of compensation under this section shall be recoverable as a civil debt.

[10

Saving for investigations by police and law enforcement officers
14. Nothing in this Act shall prohibit a police officer, a person authorised in writing by the Commissioner of Police under section 15 (1) or any other duly authorised law enforcement officer from lawfully conducting investigations pursuant to his powers conferred under any written law.

[11
[21/98]

Power of police officer to access computer and data
15. --(1) A police officer or a person authorised in writing by the Commissioner of Police shall --
(a) be entitled at any time to --
(i) have access to and inspect and check the operation of any computer to which this section applies;
(ii) use or cause to be used any such computer to search any data contained in or available to such computer; or
(iii) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such computer into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section;
(b) be entitled to require --
(i) the person by whom or on whose behalf, the police officer or investigation officer has reasonable cause to suspect, any computer to which this section applies is or has been used; or
(ii) any person having charge of, or otherwise concerned with the operation of, such computer,
to provide him with such reasonable technical and other assistance as he may require for the purposes of paragraph (a); or
(c) be entitled to require any person in possession of decryption information to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence.

[21/98]

--(2) This section shall apply to a computer which a police officer or a person authorised in writing by the Commissioner of Police has reasonable cause to suspect is or has been in use in connection with any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section.

[21/98]

(3) The powers referred to in paragraphs (a) (ii) and (iii) and (c) of subsection (1) shall not be exercised except with the consent of the Public Prosecutor.

[21/98]

(4) Any person who obstructs the lawful exercise of the powers under subsection (1) (a) or who fails to comply with a request under subsection (1) (b) or (c) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.

[21/98]

(5) For the purposes of this section --

"decryption information" means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable and incomprehensible format to its plain text version;

"encrypted data" means data which has been transformed or scrambled from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data;

"plain text version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format.

[14

[21/98]

Arrest by police without warrant

16. Any police officer may arrest without warrant any person reasonably suspected of committing an offence under this Act.

[15

Source: http://www.megalaw.com/